ARTIN'S CONJECTURE ON PRIMITIVE ROOTS

ROHAN RAMKUMAR

Abstract. Emil Artin conjectured in 1927 that any a is a primitive root modulo infinitely many primes p. Although this conjecture has not been verified for any a, in 1967, Christopher Hooley was able to prove it conditionally, assuming the generalized Riemann hypothesis. This paper will outline his proof of the conjecture, assuming some knowledge in Abstract Algebra, Galois Theory, and Algebraic Number Theory.

1. Primitive Roots

Definition 1.1. We call a a primitive root modulo n if and only if a generates $\mathbb{Z}_n^\times$, the multiplicative group of the integers modulo n.

We will consider a modulo a prime p. By Euler's theorem,

$$a^{p-1} \equiv 1 \pmod{p},$$

for all a. But, if a is a primitive root, we must have

$$\operatorname{ord}_p(a) = \left|(\mathbb{Z}/p\mathbb{Z})^\times\right| = p - 1,$$

so

$$a^{(p-1)/q} \not\equiv 1 \pmod{p}$$

for every prime $q \mid p-1$. Thus, if a is not a primitive root mod p, then for some prime q, both

$$p \equiv 1 \pmod{q}$$

and

$$a^{(p-1)/q} \equiv 1 \pmod{p}.$$

are true. We define the set $\mathscr{B}_q(a)$ to consist of primes p that satisfy both of these conditions. Also, we let $\mathscr{P}_a$ denote the set of primes p such that a is a primitive root modulo p and

$$\mathscr{P}_a(x) = \#\{p \in \mathscr{P}_a | p \leq x\}.$$

Date: June 10, 2024.

In 1927, Artin conjectured that the cardinality $\mathscr{P}_a$ is infinite for all a, and this claim is yet to be verified for any a unconditionally. However, assuming the generalized Riemann Hypothesis for Dedekind zeta functions, Hooley, in 1967, proved the following result [Hoo67]:

$$\mathscr{P}_a(x) = \delta(a)\frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right),$$

for a certain function $\delta(a)$, thus implying that the cardinality of $\mathscr{P}_a$ is infinite. This paper will outline his proof.

2. The field K_k

Proposition 2.1. *$p \in \mathscr{B}_q(a)$, if and only if p splits completely in $K_q = \mathbb{Q}(\zeta_q, a^{1/q})$.*

Proof. When $q = 2$, we have that

$$\begin{aligned} p &\equiv 1 \pmod 2 \\ a^{(p-1)/2} &\equiv 1 \pmod p, \end{aligned}$$

or that p is an odd prime and a is a quadratic residue modulo p. Considering the field $\mathbb{Q}(\sqrt{a})$, which is monogenic with minimum polynomial $x^2 - a$, by Dedekind-Kummer, since this polynomial only splits into $(x + \sqrt{a})(x - \sqrt{a})$ when a is a quadratic residue modulo p, this condition is equivalent to p splitting completely in $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\zeta_2, \sqrt{a})$, because $\zeta_2 = -1$ is already in $\mathbb{Q}$.

Otherwise, assume that $q \neq 2$ is an odd prime. Consider the polynomial

$$X^q - a.$$

Clearly, $a^{1/q}$ is a root of this polynomial, and so are $\zeta_q^i a^{1/q}$ for $0 \leq i \leq n-1$. Thus, $\mathbb{Q}(\zeta_q, a^{1/q}) = K_q$ is the splitting field of $X^q - a$. We see that since

$$\begin{aligned} N_{K_q/\mathbb{Q}}(a^{1/q}) &= \prod_{\sigma \in \operatorname{Gal} K/\mathbb{Q}} \sigma(a^{1/q}) \\ &= \prod_{i=0}^{n-1} \zeta_q^i a^{1/q} \\ &= a^{n/q}, \end{aligned}$$

where n is the degree of the field extension. Since $a^{1/q}$ is algebraic, this number must be an integer, so the degree is at least q. Since $X^q - a$

works, the degree of $\mathbb{Q}(a^{1/q})$ over $\mathbb{Q}$ is q. It can be shown ([Mar18]) through calculating the discriminant of K that

$$[\mathscr{O}_k : \mathbb{Z}[a^{1/q}]]$$

divides $q^q a^{q-1}$, hence we can apply the Dedekind-Kummer theorem on any prime $p \nmid gq$. Doing so tells us that p splits completely in $\mathbb{Q}(a^{1/q})$ if and only if

$$x^q \equiv a \pmod{p}$$

has q solutions, which happens when $p \equiv 1 \pmod{q}$, so p also splits in the cyclotomic extension $\mathbb{Q}(\zeta_q)$ and thus splits in K_q. Thus, a prime splits in K_q if and only if it is in $\mathscr{B}_q(a)$. ■

Let K_k for square-free k be the compositum of all K_q with $q \mid k$.

Lemma 2.2. *A prime splits in some K_q if and only if it splits in K_k for some square-free $k > 1$.*

Proof. This follows from the definition of completely splitting and the definition of the compositum of fields. ■

Now define

$$P_a(x, k) = \#\{p \leq x | p \text{ splits in } K_k\}$$

and

$$N_a(x, y) = \#\{p \leq x | \text{ for all } q \leq y, p \text{ does not split completely in } K_q\}.$$

We see that $\mathscr{P}_a(x) = N_a(x, x-1)$ because we cannot have

$$p \equiv 1 \pmod{q}$$

if $q \leq p$.

Lemma 2.3. *Let*

$$Q_k = \prod_{q \leq k} q.$$

Then,

$$N_a(x, k) = \sum_{l | Q_k} \mu(l) P_a(x, l).$$

Proof. We have

$$\sum_{l | Q_k} \mu(l) P_a(x, l) = \sum_{n=0}^{\pi(k)} \sum_{\omega(l)=n} (-1)^n P_a(x, l),$$

because the divisors of Q_k are square-free. If some p splits exactly m times throughout all $q \leq k$, then it is counted

$$\binom{m}{1} - \binom{m}{2} + \cdots + (-1)^{m+1}\binom{m}{m} = 1$$

times in the sum, so this is equal to $N_a(x,k)$. ■

3. The function $\delta(a)$

A very important theorem in this proof is the Chebatorev Density Theorem, which provides the density of primes that split in a certain number field, which is exactly what we need.

Theorem 3.1. *(Chebatorev Density Theorem) Let K/Q be a field extension of degree n. Then*

$$\lim_{x\to\infty} \frac{\pi_K(x)}{\pi(x)} = \frac{1}{n},$$

where π_K counts the number of prime numbers that split in K.

For each k, the density of primes that split in K_k is thus $1/n_k$, where n_k is the degree of K_k. So, to count the primes that split in no K_q, we use the principle of inclusion-exclusion, for all squarefree k, so we would expect that

$$\mathscr{P}_a(x) \sim \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{n_k}\right) \frac{x}{\log x},$$

since

$$\pi(x) \sim \frac{x}{\log x}.$$

Now, let $a = a_0 b^2$, with a_0 square-free, and let h be the largest integer such that $a^{1/h}$ is integral.

Proposition 3.2.

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{n_k} = \delta(a),$$

where

$$\delta(a) = \begin{cases} A(a) & a_0 \not\equiv 1 \pmod 4 \\ \left(1 - \mu(|a_0|) \prod_{\substack{q|a_0 \\ q|h}} \frac{1}{q-2} \prod_{\substack{q|a_0 \\ q\nmid h}} \frac{1}{q^2-q-1}\right) A(a) & a_0 \equiv 1 \pmod 4, \end{cases}$$

and

$$A(a) = \prod_{q\nmid a} \left(1 - \frac{1}{q(q-1)}\right) \prod_{q|a} \left(1 - \frac{1}{q-1}\right).$$

First, we need a formula for n_k, but before this, we need the following Lemma:

Lemma 3.3. *In a cyclic group G with order g. Then for each $m \mid g$, there is a unique subgroup of G of order m.*

Proof. Let $G = \langle a \rangle$, and consider the subgroups $\langle a^{g/m} \rangle$ for $m \mid g$. Clearly this group has order m, and for any $a^k \in G$, we can choose $m = (g, k)$, so that $a^k \in \langle a^{g/m} \rangle$, hence this subgroup is unique. ∎

Now, we can determine n_k.

Proposition 3.4.

$$n_k = \frac{k\phi(k)}{(h,k)\varepsilon(k)},$$

where

$$\varepsilon(k) = \begin{cases} 2 & 2a_0 \mid k \text{ and } a_0 \equiv 1 \pmod 4 \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Since

$$\deg(\mathbb{Q}(\zeta_k)/\mathbb{Q}) = |\operatorname{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})| = |(\mathbb{Z}/k\mathbb{Z})^\times| = \phi(k),$$

we see that

$$[K_k : \mathbb{Q}] = [K_k : \mathbb{Q}(\zeta_k)][\mathbb{Q}(\zeta_k) : \mathbb{Q}] = [K_k : \mathbb{Q}(\zeta_k)]\phi(k),$$

so let $m(k) = [K_k : \mathbb{Q}(\zeta_k)]$. First, we will show that $m(k)$ divides $k/(h,k)$. Since $x = g^{1/h}$ is an integer, we have that when $c = x^{h/(h,k)}$, then $g^{1/k} = c^{1/k_1}$, where $k_1 = k/(h,k)$. For each

$$\sigma \in \operatorname{Gal}(K_k/\mathbb{Q}(\zeta_k)),$$

define f such that

$$f(\sigma) = \sigma(c^{1/k_1})c^{k_1},$$

which is a homomorphism from $\operatorname{Gal}(K_k/\mathbb{Q}(\zeta_k))$ to $\langle \zeta_{k_1} \rangle$. Because this is a homomorphism, we must have $m(k) | k_1$.

Now, let $k_1 = m(k)\varepsilon(k)$. Since k_1 is square free, for each prime $q \mid \varepsilon(k)$, we have $q \nmid m(k)$. Since $q \mid k_1 \mid k$, the field $\mathbb{Q}(\zeta_k, a^{1/q})$ is contained in K_k, hence

$$[\mathbb{Q}(\zeta_k, c^{1/q}) : \mathbb{Q}(\zeta_k)] \mid m(k).$$

However, this degree is either q or 1, and since $q \nmid m(k)$, we must have $\mathbb{Q}(\zeta_k, c^{1/q}) = \mathbb{Q}(\zeta_k)$, so $c^{1/q}$ is contained in $\mathbb{Q}(\zeta_k)$. This can only occur when $q = 2$ because any subextension of the Galois extension $\mathbb{Q}(\zeta_k)$ must also be Galois, and this can only occur in the real field extension $\mathbb{Q}(\sqrt{a})$, with $a > 0$. Thus, the only possible prime factor of $\varepsilon(k)$ is 2. Specifically see that $a = a_0 b^2$, $\varepsilon(k) = 2$ when k is even and

$\sqrt{a_0}$ is contained in $\mathbb{Q}(\zeta_k)$, and otherwise $\varepsilon(k) = 1$. We now are left to determine for which values of a_0 the quadratic field $\mathbb{Q}(\sqrt{a_0}) \subset \mathbb{Q}(\zeta_k)$.

By Galois correspondence, each quadratic field contained in $\mathbb{Q}(\zeta_k)$ corresponds to a subgroup of index 2 of

$$\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q}) = (\mathbb{Z}/k\mathbb{Z})^\times = \prod_{p|k} (\mathbb{Z}/p\mathbb{Z})^\times,$$

by the Chinese remainder theorem and since k is square-free. When $p \neq 2$, the order of $(\mathbb{Z}/p\mathbb{Z})^\times$ is $p-1$, which is even, so there exists a unique subgroup $H \subset (\mathbb{Z}/p\mathbb{Z})^\times$ of order 2. Hence, the group

$$(\mathbb{Z}/p\mathbb{Z})^\times / H$$

is the unique subgroup of index 2 inside $(\mathbb{Z}/p\mathbb{Z})^\times$. Now, consider all possible groups

$$G = \prod_{p|k} G_p,$$

where G_p is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$) such that

$$\mathrm{lcm}\left([(\mathbb{Z}/p_1\mathbb{Z})^\times : G_{p_1}], [(\mathbb{Z}/p_2\mathbb{Z})^\times : G_{p_2}], \ldots, [(\mathbb{Z}/p_{\omega(k)}\mathbb{Z})^\times : G_{p_{\omega(k)}}]\right) = 2,$$

where $\omega(k)$ is the number of prime divisors of k. Then, each group G has index 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$, so each one corresponds to a quadratic subextension of $\mathbb{Q}(\zeta_k)$. Each G_p has index 2 or 1, and since G_2 must have index 1 because $(\mathbb{Z}/2\mathbb{Z})^\times$ has only one element, and not all G_p can have index 1, there are $2^{\omega(k)-1} - 1$ subgroups of $(\mathbb{Z}/k\mathbb{Z})^\times$) of index 2 and thus $2^{\omega(k)-1} - 1$ quadratic subextensions in $\mathbb{Q}(\zeta_k)$. Now, consider the Gauss sum

$$\tau = \sum_{a \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \left(\frac{a}{\ell}\right) \zeta_\ell^a,$$

for a prime ℓ over Jacobi symbols. Through algebraic manipulation, we see that

$$\tau^2 = \left(\frac{-1}{\ell}\right)\ell.$$

Since τ is contained in $\mathbb{Q}(\zeta_\ell)$, we have

$$\mathbb{Q}\left(\sqrt{\left(\frac{-1}{\ell}\right)\ell}\right) \subset \mathbb{Q}(\zeta_\ell).$$

By the multiplicative property of the Jacobi symbol with respect to ℓ, we can extend this to all odd divisors of k other than 1, of which there are $2^{\omega(k)-1} - 1$ many, so there are no other quadratic fields.

Thus, we see that $\mathbb{Q}(\sqrt{a_0})$ must be of the form $\mathbb{Q}\left(\sqrt{\left(\frac{-1}{\ell}\right)\ell}\right)$ in order for the field to be contained inside $\mathbb{Q}(\zeta_k)$. This occurs when either $a_0 > 0$ and $\left(\frac{-1}{a_0}\right) = 1$ or $a_0 < 0$ and $\left(\frac{-1}{|a_0|}\right) = -1$. In both cases, we have

$$a_0 \equiv 1 \pmod 4.$$

Thus, we have

$$\varepsilon(k) = \begin{cases} 2 & 2a_0 \mid k \text{ and } a_0 \equiv 1 \pmod 4 \\ 1 & \text{otherwise.} \end{cases}$$

■

Before we continue, we need another Lemma:

Lemma 3.5. *For $n \geq 1$, we have $\phi(n) \geq \sqrt{\frac{n}{2}}$.*

Proof. It is known (page 267 of [HW75]) that for the largest primorial

$$Q_k = \prod_{l=0}^{k} q_l$$

with $q_k - 1 \leq q_k^{1-\delta}$,

$$\inf\left\{\frac{\phi(n)}{n^{1-\delta}} : n \in \mathbb{N}\right\} = \frac{\phi(Q_k)}{Q_k}.$$

When $\delta = \frac{1}{2}$, we see that $2 - 1 \leq \sqrt{2}$ and $3 - 1 > \sqrt{3}$, so $q_k = 2$, and

$$\frac{\phi(n)}{\sqrt{n}} \geq \frac{\phi(2)}{\sqrt{2}} = \frac{1}{\sqrt{2}},$$

so

$$\phi(n) \geq \sqrt{\frac{n}{2}}$$

for all $n \geq 1$. ■

Now we can prove that

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{n_k} = \delta(a).$$

Proof. When $a_0 \not\equiv 1 \pmod 4$, we have

$$\begin{aligned}\sum_{k=1}^{\infty} \frac{\mu(k)}{n_k} &= \sum_{k=1}^{\infty} \frac{\mu(k)(h,k)\varepsilon(k)}{k\phi(k)} \\ &= \prod_q \left(1 + \frac{\mu(q)(h,q)}{q\phi(q)}\right) \\ &= \prod_q \left(1 + \frac{(h,q)}{q(q-1)}\right) \\ &= \prod_{q\mid h} \left(1 - \frac{1}{q-1}\right) \prod_{q\nmid h} \left(1 - \frac{1}{q(q-1)}\right) \\ &= A(a) \\ &= \delta(a).\end{aligned}$$

This works because

$$\sum_{k=1}^{\infty} \left|\frac{\mu(k)(h,k)}{k\phi(k)}\right| = \sum_{k=1}^{\infty} \frac{(h,k)}{k\phi(k)} \leq \sum_{k=1}^{\infty} \frac{h\sqrt{2}}{k^{3/2}}$$

is bounded.

If $a_0 \equiv 1 \pmod 4$, then

$$\begin{aligned}\sum_{k=1}^{\infty} \frac{\mu(k)(h,k)\varepsilon(k)}{k\phi(k)} &= \sum_{2a_0\nmid k} \frac{\mu(k)(h,k)\varepsilon(k)}{k\phi(k)} + 2\sum_{2a_0\mid k} \frac{\mu(k)(h,k)\varepsilon(k)}{k\phi(k)} \\ &= A(a) - A(a)\mu(|a_0|) \prod_{\substack{q\mid a_0 \\ q\mid h}} \frac{1}{q-2} \prod_{\substack{q\mid a_0 \\ q\nmid h}} \frac{1}{q^2-q-1} \\ &= \delta(a)\end{aligned}$$

after heavy algebraic manipulation. ∎

4. Finding the Error Bound

Chebotarev's density theorem unconditionally is not strong enough to prove Artin's conjecture, since it does not provide an error bound on the asymptotic density. However, by assuming the Generalized Riemann Hypothesis for a Dedekind zeta function ζ_K of some field $K/\mathbb{Q}$, we have the following conditional result [GM19]:

Theorem 4.1. *(Explicit Chebotarev Density Theorem) If $\pi_K(x)$ is the number of primes less than or equal to x that completely split in K,*

then

$$\pi_K(x) = \frac{\mathrm{Li}(x)}{[K:\mathbb{Q}]} + O(\sqrt{x}\log x) + O\left(\frac{\sqrt{x}\log \Delta_K}{[K:\mathbb{Q}]}\right),$$

assuming the Generalized Riemann Hypothesis for ζ_K.

Applying this result on $P_a(x,k)$ and bounding

$$\frac{\log|\Delta_{K_k}|}{[K_k:\mathbb{Q}]} = O(\log k),$$

we get

$$P_a(x,k) = \frac{\mathrm{Li}(x)}{n_k} + O(\sqrt{x}\log(kx)),$$

and we are finally ready to bound the $\mathscr{P}_a(x)$.

Now, we will define

$$M_a(x,y,z) = \#\{p \le x | p \text{ splits completely in any } K_q, y \le q \le z\}.$$

We see that for any ξ_1,

$$\mathscr{P}_a(x) \le N_a(x,\xi_1).$$

Also,

$$N_a(x,\xi_1) - M_a(x,\xi_1,x-1) \le \mathscr{P}_a(x)$$

because it takes care of the overestimates of N_a if $\xi_1 < x-1$. So, $\mathscr{P}_a(x) = N_a(x,\xi_1) + O(M_a(x,\xi_1,x-1))$. In order to refine an estimate on M_a, we will split the range ξ_1 to $x-1$ into three ranges; specifically:

$$M_a(x,\xi_1,x-1) \le M_a(x,\xi_1,\xi_2) + M_a(x,\xi_2,\xi_3) + M_a(x,\xi_3,x-1),$$

where, for large enough x,

$$\xi_1 = \frac{1}{6}\log x, \xi_2 = \sqrt{x}\log^{-2} x, \xi_3 = \sqrt{x}\log x.$$

First, we have

$$\begin{aligned} N_a(x,\xi_1) &= \sum_l \mu(l) P_a(x,l) \\ &= \sum_l \frac{\mu(l)}{n_l}\mathrm{Li}(x) + O\left(\sum_{l\le\xi_1}\sqrt{x}\log x\right) \\ &= \left(\sum_l \frac{\mu(l)}{n_l}\right)\mathrm{Li}(x) + O\left(\frac{x}{\log^2 x}\right) \\ &= \left(\sum_{k=1}^{\infty}\frac{\mu(k)}{n_k}\right)\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right), \end{aligned}$$

from integration by parts on Li and bounding the error term

$$\sum_{\substack{\exists q|k \\ q>\xi_1}} \frac{\mu(k)}{n_k} = O\left(\sum_{q>\xi_1} \frac{1}{q(q-1)}\right) O\left(\frac{1}{\xi_1}\right),$$

because

$$\prod_{q\leq\xi_1} q \leq 2^{2\xi_1} \leq e^{2\xi_i} \leq x^{1/3}.$$

Moving to the next term, we have

$$M_a(x,\xi_1,\xi_2) = \sum_{\xi_1\leq q\leq\xi_2} P_a(x,q),$$

because the right side overcounts when some $p \leq x$ splits in more than one K_q. Estimating this, we have

$$\begin{aligned}\sum_{\xi_1\leq q\leq\xi_2} P_a(x,q) &= \sum_{\xi_1\leq q\leq\xi_2} \left(\frac{\mathrm{Li}(x)}{n_q} + O(\sqrt{x}\log(qx)\right) \\ &= O\left(\mathrm{Li}(x)\sum_{q>\xi_1}\frac{1}{q(q-1)}\right) + O(\sqrt{x}\log x\pi(\xi_1)) \\ &= O\left(\frac{x}{\log^2 x}\right).\end{aligned}$$

For the next term, $M_a(x,\xi_2,\xi_3)$, it suffices to use the weaker condition that counts p such that $p \equiv 1 \pmod q$:

$$\begin{aligned}M_a(x,\xi_2,\xi_3) &\leq \sum_{\xi_1\leq q\leq\xi_2} \pi(x;q,1) \\ &\leq \sum_{\xi_2\leq q\leq\xi_3} \frac{2x}{(q-1)\log(x/q)}\end{aligned}$$

by the Brun-Titchmarsh theorem [MV73]. Continuing, we have

$$\begin{aligned}\sum_{\xi_2\leq q\leq\xi_3} \frac{2x}{(q-1)\log(x/q)} &= O\left(\frac{x}{\log x}\sum_{\xi_2\leq q\leq\xi_3}\frac{1}{q}\right) \\ &= O\left(\frac{x}{\log^2 x}\sum_{\xi_2\leq q\leq\xi_3}\frac{\log q}{q}\right) \\ &= O\left(\frac{x}{\log^2 x}\left(\frac{\xi_3}{\xi_2}+O(1)\right)\right) \\ &= O\left(\frac{x\log\log x}{\log^2 x}\right).\end{aligned}$$

by a theorem of Mertens [Mer74]. Finally, for the third term, we will use the weaker condition that

$$a^{\frac{2(p-1)}{q}} \equiv 1 \pmod{p},$$

and since $q > \sqrt{x}\log x$ and $p \leq x$, we have

$$\frac{p-1}{q} < \frac{x}{\log x}.$$

So, the product of all p counted by $M_a(x, \xi_3, x-1)$ must divide

$$\prod_{m<\frac{x}{\log x}} (a^{2m}-1) < \prod_{m<\frac{x}{\log x}} a^{2m}.$$

Since all primes are at least 2, we have

$$M_a(x, \xi_3, x-1) < \log_2 \left(\prod_{m<\frac{x}{\log x}} a^{2m} = \frac{2\log a}{\log 2} \sum_{m<\frac{x}{\log x}} m. \right)$$

Since

$$\sum_{m<N} m = \frac{1}{2}N(N-1) = O(N^2),$$

we get

$$M_a(x, \xi_3, x-1) = O\left(\frac{x}{\log^2 x}\right).$$

Combining these sums, we get

$$\mathscr{P}_a(x) = \delta(a)\frac{x}{\log x} + O\left(\frac{x\log\log x}{\log^2 x}\right),$$

thus proving Artin's conjecture assuming the generalized Riemann hypothesis.

5. Conclusion

Although Artin's conjecture is yet to be verified for a specific a, Heath-Brown proved in 1986 that at least one of $2, 3$ or 5 is a primitive root modulo infinitely many primes, and that there can only be at most two prime values of a for which Artin's conjecture is not true [HB86]. In a similar vein to Artin's Conjecture, Lang and Trotter in [LT77] conjectured a similar statement for when a point on an elliptic curve generates the entire set of points modulo p, and this conjecture was again proved conditionally for specific curves that have complex multiplication, again assuming the generalized Riemann hypothesis [GRM86].

References

[GM19] Loïc Grenié and Giuseppe Molteni. An explicit chebotarev density theorem under grh. *Journal of Number Theory*, 200:441–485, 2019.

[GRM86] Rajiv Gupta and M. Ram Murty. Primitive points on elliptic curves. *Compositio Mathematica*, 58(1):13–44, 1986.

[HB86] D. R. Heath-Brown. Artin's conjecture for primitive roots. *The Quarterly Journal of Mathematics*, 37(1):27–38, 1986.

[Hoo67] Christopher Hooley. On artin's conjecture. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1967(225):209–220, January 1967.

[HW75] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford, fourth edition, 1975.

[LT77] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bulletin of the American Mathematical Society*, 83(2):289–292, 1977.

[Mar18] Daniel A. Marcus. *Number Fields*. Springer International Publishing, 2018.

[Mer74] Franz Mertens. Ein beitrag zur analytischen zahlentheorie. *Journal für die reine und angewandte Mathematik*, 78:46–62, 1874.

[MV73] H. L. Montgomery and R. C. Vaughan. The large sieve. *Mathematika*, 20(2):119–134, December 1973.